Single Connect Kron

Datasheet

UNIFIED ACCESS MANAGER

Unified Access Manager provides built-in and pre-integrated TACACS+ and RADIUS servers that provide AAA (Authentication, Authorization and Accounting) services for network infrastructure and also **extends authentication, single-sign-on capabilities and policy configurations of Active Directory to network infrastructure.**

With countless network devices to manage, organization's **IT departments** need to implement policies to **determine** and control who can log in to manage each device, what operations they can run, and log all actions. Security incidents or errors that result in loss of service and network **downtime** can easily occur while managing these policies separately on each device. As compliance requirements and **security** standards require using standardized tools to centralize authentication for **administrative** management, many IT departments choose to use AAA (Authentication, Authorization and Accounting) protocols, RADIUS or TACACS+ to address these issues, as these protocols enable the organization to have all network devices managed by a single platform.

The Ideal Replacement for Cisco's Access Control Server

As the defacto industry standard for device network authentication and administration, Cisco's Access Control Server (ACS) has been deployed around the world, and with the combination of TACACS+ and RADIUS authentication services, served the needs of many customers for a long time. With the EOL announcement, organizations are taking the opportunity to evaluate alternatives and have found that KRON Single Connect™ is the only credible alternative in the marketplace. Many enterprises have already chosen to replace ACS with Kron Single Connect. You can learn more about this by reading our announcements about our customers.

Single Connect™ provides more comprehensive functionality than Cisco ACS and ISE. Implementation easily leverages current ACS configurations. The cost model (resources and licenses) for Single Connect is 40-60% less than a traditional ISE upgrade and the time-to-value is significantly reduced.

After Cisco announced the end of life for its ACS (Access Control System) product, it offered to migrate their customers from Cisco ACS to Cisco ISE (Identity Service Engine). However, Cisco ISE is originally designed for Network Access, not for Network Administration, and although it offers RADIUS/TACACS+ protocol support, it does NOT support any other Privileged Access Management features, such as RDP/HTTP/SFTP/SQL session management, Dynamic Password Controller, Application-to-Application Password Management or Multi-Factor Authentication. So, from a SecOps point of view, migrating from Cisco ACS to Cisco ISE means using it as a Network Access Management tool (wireless network access, bring your own devices, guest users, etc.).

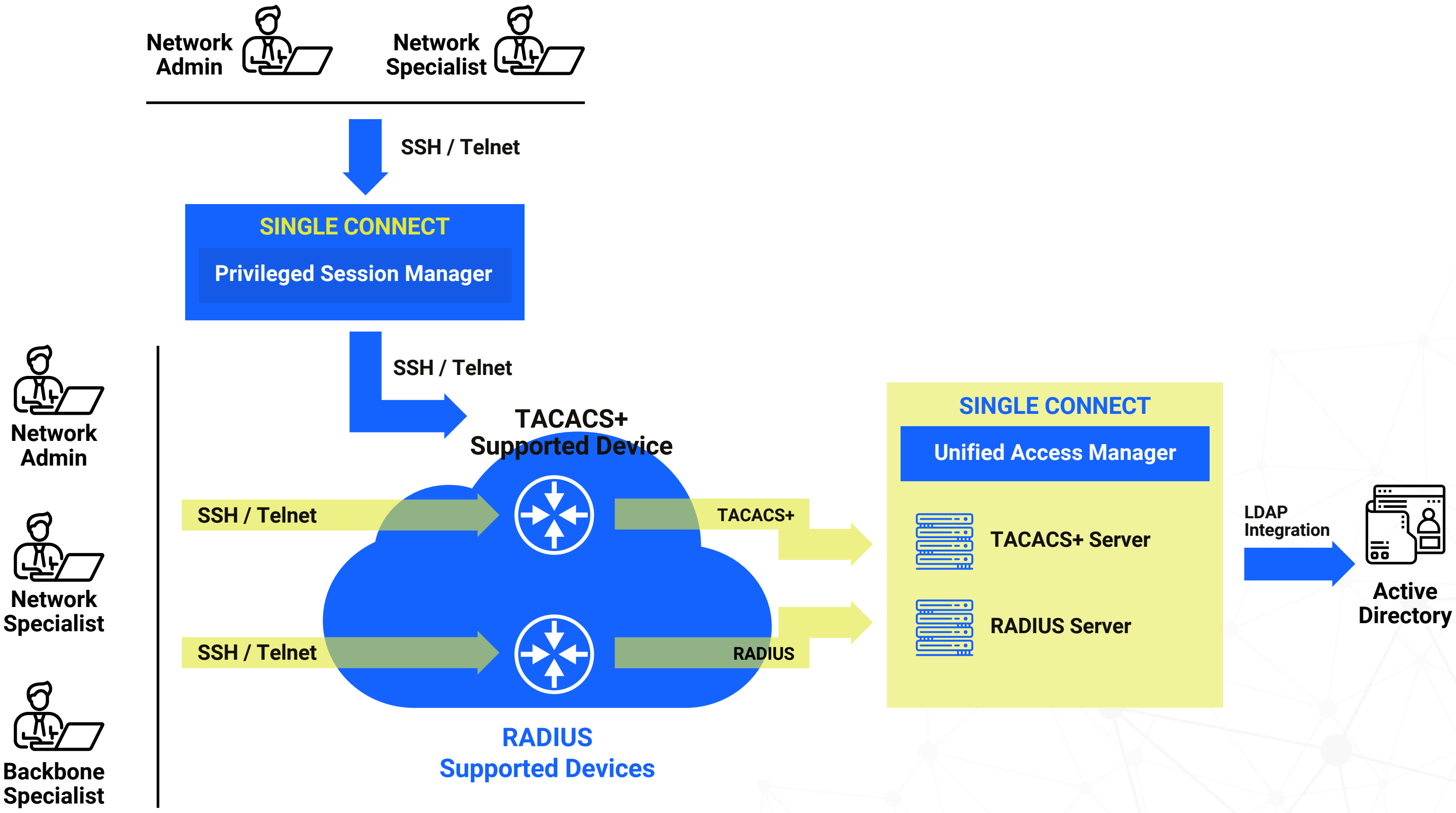
Most of the time SecOps teams are not interested in Network Access, either because they already have a product for that purpose, or it is not under their scope. However, SecOps are very much interested in PAM tools.

Single Connect Kron

Datasheet

HOW UNIFIED ACCESS MANAGER WORKS

In large enterprise networks, the task of administering passwords on each device can be simplified by doing the user authentication centrally on a server.



TACACS+ or RADIUS is an access control protocol that allow a switch to authenticate all login attempts through a central authentication server. The network administrator configures the switch with the address of that authentication server, and switch and server exchange messages to authenticate each user before allowing access to the management console.

TACACS+ or RADIUS server consists of three services: authentication, authorization and accounting. Authentication is the action of determining who the user is and whether her or she is allowed access to the switch Authorization is the action of determining what the user is allowed to do on the system. Accounting is the action of collecting data related to resource usage.

Authentication

Step 1: The user initiates a CLI session towards the target device. The user enters a username & password.

Step 2: The target device sends the username & password to the TACACS+ Access Manager.

Step 3: Successful response if the username & password are correct.

Step 4: The target device sends the response to the user.

Step 5: A CLI session between the user and the target device is established. The user can now enter commands for device administration purposes.

Administration

Step 6: The user enters a command on his CLI screen. It is sent to the target device.

Step 7: The target device sends the command to the TACACS+Access Manager.

Step 8: The TACACS+ Access Manager

- Checks whether the user has the right/privilege to run that command.
- Respond either accept or reject.
- Logs the command along with the response.

Step 9: If the TACACS+Access Manager responds with an accept message, the target device runs the command and sends the response to the user. If the response was a reject message, the target device sends a fail message to the user.

Single Connect Kron

Datasheet

FEATURES & BENEFITS

Stand-alone AAA Solution - Native built-in TACACS+ and **RADIUS** servers support, no need for additional platform to replace aging Cisco ACS servers.

Full visibility, detailed **audit** logs. All commands, either failed or succeeded, are indisputably logged, creating a record of which user attempted to run which command on which device and when. Centralized **visibility** of all user sessions and executed commands in searchable, indexed human readable format.

“Separation of duties” and “least privilege” best practices are achieved, regardless of the role/profile capabilities of the device. Single Connect **TACACS+** Access Manager enables any custom policies (allowed command sets, blocked command sets) to be defined and applied to any user group, ensuring that only the “required set of commands” can be executed by a user to fulfill his tasks, and no other command execution is allowed at all.

Extend Active Directory group policies to network infrastructure and support compliance with regulations including GDPR, ISO 27001, SOX, HIPAA, PCI.

Controls direct and console access to target devices, Single Connect TACACS+ Access Manager can enforce users to connect to devices through Single Connect **PSM** to having enhanced features on session control.

Enable **multi-factor** authentication for network infrastructure, in combination with Single Connect MFA Manager.

Eliminates weak passwords and/or **non-expiry** passwords.

Enables the definition of **time-based** access limitations. Based on time of day, day of the week, maintenance-window hours, etc.

Disables inactive **privileged** accounts.

Multi-tenant. On a single TACACS+ Access Manager instance, while keeping the governance of the entire network in place, each **enterprise department/ region** can be assigned limited privileges to manage their own devices, isolated from the larger network.

Log users onto network devices using their Active Directory (AD) usernames and passwords, without additional infrastructure or password **synchronization** requirements, simplifying administration.

Auto lock user account when an employee terminates employment. Integration with enterprise **Active Directory** (or LDAP) is required.

Open protocol based, **no vendor** lock-in, supporting virtually all network devices.

Single Connect TACACS+ & RADIUS Access Manager supports configuration of custom **AVP** (Attribute Value Pair).

Highly scalable. Supports up to 250,000 devices in a single instance.